

We claim:

1 **1.** A method for tracing a sequence of packets to a potential source thereof within a
2 communications network, the sequence of packets being received at a target host in said
3 communications network at a received packet rate, the method comprising the steps of:
4 applying a burst load to each of one or more selected network elements in said
5 communications network;
6 for each selected network element, measuring a change in said received packet
7 rate in response to said application of said burst load to said selected network element;
8 and
9 determining said potential source of said sequence of packets based on said
10 measured changes in said received packet rate.

1 **2.** The method of claim 1 wherein said communications network comprises the
2 Internet.

1 **3.** The method of claim 1 wherein each of said selected network elements
2 comprises a network link.

1 4. The method of claim 3 wherein said step of applying a burst load to said
2 network link comprises transmitting packets to a subnetwork of said communications
3 network to initiate a responsive flow of packets through said network link.

1 **5.** The method of claim 4 wherein said transmitted packets are spoofed from an
2 end of said network link closest to said target host.

1 **6.** The method of claim 4 wherein said transmitted packets comprise UDP chargen
2 requests.

1 7. The method of claim 1 wherein each of said selected network elements
2 comprises a network router.

1 8. The method of claim 1 further comprising the step of generating a map
2 comprising routes from said target host to a plurality of subnetworks of said
3 communications network.

1 9. The method of claim 1 further comprising the step of eliminating said selected
2 network element from consideration as said potential source of said sequence of packets
3 when said change in said received packet rate meets a predetermined criterion.

1 10. The method of claim 9 wherein said predetermined criterion comprises a
2 determination of whether said change in said received packet rate is less than a
3 predetermined threshold.

1 11. The method of claim 9 wherein said step of eliminating said selected network
2 element from consideration also eliminates from consideration one or more
3 subnetworks of said communications network which are connected to said selected
4 network element.

1 12. The method of claim 1 wherein said sequence of packets comprises a Denial-of-
2 Service attack on said target host.

1 13. The method of claim 1 wherein said steps of applying said burst load, measuring
2 said changes in said received packet rate, and determining said potential source of said
3 sequence of packets, are executed under the control of an automated algorithm.

1 14. The method of claim 1 wherein said steps of applying said burst load and
2 determining said potential source of said sequence of packets, are executed under the at
3 least partial control of a human operator.

1 **15.** The method of claim 14 further comprising the step of displaying information,
2 said information including data representative of said measured changes in said
3 received packet rate, to said human operator, for use by said human operator in
4 exercising said at least partial control.

1 **16.** An apparatus for tracing a sequence of packets to a potential source thereof
2 within a communications network, the sequence of packets being received at a target
3 host in said communications network at a received packet rate, the apparatus
4 comprising:
5 means for applying a burst load to each of one or more selected network
6 elements in said communications network;
7 means for measuring changes in said received packet rate in response to said
8 application of said burst load to each of said selected network elements; and
9 means for determining said potential source of said sequence of packets based
10 on said measured changes in said received packet rate.

1 **17.** The apparatus of claim 16 wherein said communications network comprises the
2 Internet.

1 **18.** The apparatus of claim 16 wherein each of said selected network elements
2 comprises a network link.

1 **19.** The apparatus of claim 18 wherein said means for applying a burst load to said
2 network link comprises means for transmitting packets to a subnetwork of said
3 communications network to initiate a responsive flow of packets through said network
4 link.

1 **20.** The apparatus of claim 19 wherein said transmitted packets are spoofed from an
2 end of said network link closest to said target host.

09501286-070901

- 1 **21.** The apparatus of claim 19 wherein said transmitted packets comprise UDP
2 chargen requests.
- 1 **22.** The apparatus of claim 16 wherein each of said selected network elements
2 comprises a network router.
- 1 **23.** The apparatus of claim 16 further comprising means for generating a map
2 comprising routes from said target host to a plurality of subnetworks of said
3 communications network.
- 1 **24.** The apparatus of claim 16 further comprising means for eliminating said
2 selected network element from consideration as said potential source of said sequence
3 of packets when said change in said received packet rate meets a predetermined
4 criterion.
- 1 **25.** The apparatus of claim 24 wherein said predetermined criterion comprises a
2 determination of whether said change in said received packet rate is less than a
3 predetermined threshold.
- 1 **26.** The apparatus of claim 24 wherein said means for eliminating said selected
2 network element from consideration also eliminates from consideration one or more
3 subnetworks of said communications network which are connected to said selected
4 network element.
- 1 **27.** The apparatus of claim 16 wherein said sequence of packets comprises a Denial-
2 of-Service attack on said target host.
- 1 **28.** The apparatus of claim 16 wherein said means for applying said burst load, said
2 means for measuring said changes in said received packet rate, and said means for

